Prop Let \( \mathcal{A} \colon \{ I \} \) be any family of subgroups of \( G \). Then the intersection \( \bigcap_{i \in I} H_i \) is a subgroup of \( G \).

**Proof:** Let \( x, y \in \bigcap_{i \in I} H_i \).

I.e., \( x, y \in H_i \) \( \forall i \in I \).

Thus \( xy^{-1} \in H_i \) \( \forall i \in I \) (\( H_i \) subgroup).

\( \Rightarrow xy^{-1} \in \bigcap_{i \in I} H_i \).

So \( \bigcap_{i \in I} H_i \subseteq G \)

let \( X \subseteq G \) be any subset
The subgroup generated by \( x \), written \( \langle x \rangle \), is defined to be the intersection of all subgroups \( H \leq G \) containing the set \( x \);

\[
\langle x \rangle = \bigcap \{ H \leq G \mid x \in H \}
\]

Notice that \( \langle x \rangle \) is a subgroup (by the previous Proposition) containing \( x \) and if \( H \) is any subgroup containing \( x \), then \( \langle x \rangle \leq H \). Thus \( \langle x \rangle \) is the smallest subgroup of \( G \) containing \( x \).

In case \( x = \exists x^2 \), then \( \langle x \rangle \) is the cyclic subgroup \( \langle x \rangle \) generated by \( x \), (because any subgroup containing \( x \) must contain all powers \( x^n \) of \( x \)).
If \( X \) is any set, then we can describe all elements of the subgroup \( \langle X \rangle \) generated by \( X \). If \( X = \emptyset \) then \( \langle X \rangle = \{ e \} \) is the trivial group, so take \( X = \emptyset \).

A word on \( X \) is an element
\[
e^1, \ldots, x^n, x^m \in G
\]

where \( e = 1 \), \( x \in X \), \( n \) any pos. integer.

Then \( \langle X \rangle \) is the set of all words on \( X \). (check)

Cyclic Groups

Define: A group \( G \) is cyclic if there exists an element \( g \in G \) such that \( G = \langle g \rangle \).

Example: \( \mathbb{Z} \) is cyclic with generator 1. It has infinite order.
Prop 2: If the unique cyclic group of infinite order, that is, if $G = \langle x \rangle$, where $x$ has infinite order, then we have an isomorphism

$$\phi: \mathbb{Z} \rightarrow \langle x \rangle$$

$$n \mapsto x^n$$

Proof: The function $\phi$ is a homomorphism

Since $\phi(a + b) = x^{a+b} = x^a \cdot x^b = \phi(a) \cdot \phi(b)$

It is surjective by the definition of $\langle x \rangle$.

It remains to show it is injective.

Suppose $\phi(a) = \phi(b)$. Then $x^a = x^b$

$$\Rightarrow x^{a-b} = 1$$

As $x$ has infinite order, this implies $a = b$ (else $x^{a-b}$ for some $n > 0$).

So $\phi$ is injective.
Finite subgroups can be characterized entirely in terms of their order.

**Proposition**

Let $G = \langle x \rangle$ and $H = \langle y \rangle$ be two cyclic groups with $|x| = |y|$. Then we have an isomorphism $\varphi : G \to H$ such that $x^k \mapsto y^n$, for $n \leq |x| - 1$.

**Proof**

Recall that $G = \{1, x, \ldots, x^{\frac{|x|-1}{2}}\}$ and $H = \{1, y, \ldots, y^{\frac{|y|-1}{2}}\}$.

We see that $\varphi$ is bijective. To show it is a homomorphism, firstly let $n \in \mathbb{Z}$ be an integer and write $n = m|x| + r$, $0 \leq r < |x|$. Then

\[x^n = (x^{|x|})^m x^r = y^{m|x|} x^r = y^n x^r\]
Then \( f(x^n) = f(x^r) = y^n = y^r \)

valid for any \( n \in \mathbb{Z} \)

Thus \( f(x^n \cdot x^m) = f(x^{n+m}) = y^{n+m} = y^n \cdot y^m \)

\( = f(x^n) \cdot f(x^m) \)

Notice that groups of order \( n \) exist for any \( n \geq 0 \):
\[ \exists \mathbb{Z}_{m(\mathbb{Z}_n)} \mid m \in \mathbb{Z} \geq f \]

is a group of order \( n \)

We write the cyclic group as \( \mathbb{Z}_n \).

If \( a, b \in \mathbb{Z} \) and \( d = \gcd(a, b) \) is their gcd,

then \( d = ra + sb \) for integers \( r, s \) by the Euclidean algorithm.
The following proposition describes the order of any element of a cyclic group. First we need:

**Lemma.**

Let $G = \langle x \rangle$ be a cyclic group and $n = |x| < \infty$. Suppose $x^m = 1$. Then $n$ divides $m$.

**Proof.** Set $d = \gcd(n, m)$.

So $d = mn + sm$ \quad \text{where } s \in \mathbb{Z}$

$x^d = x^m \cdot x^{sm} = 1$

As $d \mid n$ we have done by the definition of $|x|$.

Thus let $G = \langle x \rangle$ be a cyclic group and $n = |x| < \infty$. Then $|x^m| = \frac{n}{\gcd(m,n)}$. 

pf Let \( d = \gcd(m, n) \)

\[ m = ad \quad n = bd \quad \text{for} \]

coprime integers \( a, b \). So \( b = \frac{n}{\gcd(m, n)} \)

we have \( x^m b = x^{ad} b = x^{ad} \)

\[ (x^m)^b = x^b = x^{an} = 1 \]

Thus, the lemma above \( |x^m| \) divide \( b \).

Set \( c = |x^m| \)

Then \( 1 = x^m \cdot c \quad \Rightarrow \quad |x| \quad \text{divide} \quad mc \)

\[ n \mid mc \quad \Rightarrow \quad b \mid ac \]

\[ bd = ad \cdot c \]

As \( \gcd(a, b) = 1 \) this implies \( b \mid (x^m) \)

Thus \( |x^m| = b \quad (a, \ b, \ |x^m| = b \quad \text{as well}) \)

as required.